AppleJeus: Analysis of North Korea's Cryptocurrency Malware | CISA

Published: 2021-04-15 · Archived: 2026-04-05 12:40:04 UTC

Summary

This Advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.

This joint advisory is the result of analytic efforts among the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Treasury (Treasury) to highlight the cyber threat to cryptocurrency posed by North Korea, formally known as the Democratic People's Republic of Korea (DPRK), and provide mitigation recommendations. Working with U.S. government partners, FBI, CISA, and Treasury assess that Lazarus Group—which these agencies attribute to North Korean state-sponsored advanced persistent threat (APT) actors—is targeting individuals and companies, including cryptocurrency exchanges and financial service companies, through the dissemination of cryptocurrency trading applications that have been modified to include malware that facilitates theft of cryptocurrency.

These cyber actors have targeted organizations for cryptocurrency theft in over 30 countries during the past year alone. It is likely that these actors view modified cryptocurrency trading applications as a means to circumvent international sanctions on North Korea—the applications enable them to gain entry into companies that conduct cryptocurrency transactions and steal cryptocurrency from victim accounts. As highlighted in FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks and Guidance on the North Korean Cyber Threat, North Korea's state-sponsored cyber actors are targeting cryptocurrency exchanges and accounts to steal and launder hundreds of millions of dollars in cryptocurrency.[1][2][3] The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity, visit https://www.us-cert.cisa.gov/northkorea.

The U.S. Government has identified malware and indicators of compromise (IOCs) used by the North Korean government to facilitate cryptocurrency thefts; the cybersecurity community refers to this activity as "AppleJeus." This report catalogues AppleJeus malware in detail. North Korea has used AppleJeus malware posing as cryptocurrency trading platforms since at least 2018. In most instances, the malicious application—seen on both Windows and Mac operating systems—appears to be from a legitimate cryptocurrency trading company, thus fooling individuals into downloading it as a third-party application from a website that seems legitimate. In addition to infecting victims through legitimate-looking websites, HIDDEN COBRA actors also use phishing, social networking, and social engineering techniques to lure users into downloading the malware.

Refer to the following Malware Analysis Reports (MARs) for full technical details of AppleJeus malware and associated IOCs.

- MAR-10322463-1.v1: AppleJeus – Celas Trade Pro

- MAR-10322463-2.v1: AppleJeus – JMT Trading
- MAR-10322463-3.v1: AppleJeus – Union Crypto
- MAR-10322463-4.v1: AppleJeus – Kupay Wallet
- MAR-10322463-5.v1: AppleJeus – CoinGoTrade
- MAR-10322463-6.v1: AppleJeus – Dorusio
- MAR-10322463-7.v1: AppleJeus – Ants2Whale

Click here for a PDF version of this report.

Technical Details

The North Korean government has used multiple versions of AppleJeus since the malware was initially discovered in 2018. This section outlines seven of the versions below. The MARs listed above provide further technical details of these versions. Initially, HIDDEN COBRA actors used websites that appeared to host legitimate cryptocurrency trading platforms to infect victims with AppleJeus; however, these actors are now also using other initial infection vectors, such as phishing, social networking, and social engineering techniques, to get users to download the malware.

Targeted Nations

HIDDEN COBRA actors have targeted institutions with AppleJeus malware in several sectors, including energy, finance, government, industry, technology, and telecommunications. Since January 2020, the threat actors have targeted these sectors in the following countries: Argentina, Australia, Belgium, Brazil, Canada, China, Denmark, Estonia, Germany, Hong Kong, Hungary, India, Ireland, Israel, Italy, Japan, Luxembourg, Malta, the Netherlands, New Zealand, Poland, Russia, Saudi Arabia, Singapore, Slovenia, South Korea, Spain, Sweden, Turkey, the United Kingdom, Ukraine, and the United States (figure 1).

Figure 1: Countries targeted with AppleJeus by HIDDEN COBRA threat actors since 2020

AppleJeus Versions Note

The version numbers used for headings in this document correspond to the order the AppleJeus campaigns were identified in open source or through other investigative means. These versions may or may not be in the correct order to develop or deploy the AppleJeus campaigns.

AppleJeus Version 1: Celas Trade Pro

Introduction and Infrastructure

In August 2018, open-source reporting disclosed information about a trojanized version of a legitimate cryptocurrency trading application on an undisclosed victim's computer. The malicious program, known as Celas Trade Pro, was a modified version of the benign Q.T. Bitcoin Trader application. This incident led to the victim company being infected with a Remote Administration Tool (RAT) known as FALLCHILL, which was attributed to North Korea (HIDDEN COBRA) by the U.S. Government. FALLCHILL is a fully functional RAT with multiple commands that the adversary can issue from a command and control (C2) server to infected systems via

various proxies. FALLCHILL typically infects a system as a file dropped by other HIDDEN COBRA malware (*Develop Capabilities: Malware* [T1587.001]). Because of this, additional HIDDEN COBRA malware may be present on systems compromised with FALLCHILL.[4]

Further research revealed that a phishing email from a Celas LLC company (*Phishing: Spearphishing Link* [T1566.002]) recommended the trojanized cryptocurrency trading application to victims. The email provided a link to the Celas' website, `celasllc[.]com` (*Acquire Infrastructure: Domain* [T1583.001]), where the victim could download a Windows or macOS version of the trojanized application.

The `celasllc[.]com` domain resolved to the following Internet Protocol (IP) addresses from May 29, 2018, to January 23, 2021.

- `45.199.63[.]220`
- `107.187.66[.]103`
- `145.249.106[.]19`
- `175.29.32[.]160`
- `185.142.236[.]213`
- `185.181.104[.]82`
- `198.251.83[.]27`
- `208.91.197[.]46`
- `209.99.64[.]18`

The `celasllc[.]com` domain had a valid Sectigo (previously known as Comodo) Secure Sockets Layer (SSL) certificate (*Obtain Capabilities: Digital Certificates* [T1588.004]). The SSL certificate was "Domain Control Validated," a weak security verification level that does not require validation of the owner's identity or the actual business's existence.

Celas Trade Pro Application Analysis

Windows Program

The Windows version of the malicious Celas Trade Pro application is an MSI Installer (`.msi`). The MSI Installer installation package comprises a software component and an application programming interface (API) that Microsoft uses for the installation, maintenance, and removal of software. The installer looks legitimate and is signed by a valid Sectigo certificate that was purchased by the same user as the SSL certificate for celasllc[.]com (*Obtain Capabilities: Code Signing Certificates* [T1588.003]). The MSI Installer asks the victim for administrative privileges to run (*User Execution: Malicious File* [T1204.002]).

Once permission is granted, the threat actor is able to run the program with elevated privileges (*Abuse Elevation Control Mechanism* [T1548]) and MSI executes the following actions.

- Installs `CelasTradePro.exe` in folder `C:\Program Files (x86)\CelasTradePro`
- Installs `Updater.exe` in folder `C:\Program Files (x86)\CelasTradePro`
- Runs `Updater.exe` with the `CheckUpdate` parameters

The `CelasTradePro.exe` program asks for the user's exchange and loads a legitimate-looking cryptocurrency trading platform—very similar to the benign Q.T. Bitcoin Trader—that exhibits no signs of malicious activity.

The `Updater.exe` program has the same program icon as `CelasTradePro.exe`. When run, it checks for the `CheckUpdate` parameter, collects the victim's host information (*System Owner/User Discovery* [T1033]), encrypts the collected information with a hardcoded XOR encryption, and sends information to a C2 website (*Exfiltration Over C2 Channel* [T1041]).

macOS X Program

The macOS version of the malicious application is a DMG Installer that has a disk image format that Apple commonly uses to distribute software over the internet. The installer looks legitimate and has a valid digital signature from Sectigo (*Obtain Capabilities: Digital Certificates* [T1588.004]). It has very similar functionality to the Windows version. The installer executes the following actions.

- Installs `CelasTradePro` in folder `/Applications/CelasTradePro.app/Contents/MacOS/`
- Installs `Updater` in folder `/Applications/CelasTradePro.app/Contents/MacOS`
- Executes a `postinstall` script
    - Moves `.com.celastradepro.plist` to folder `LaunchDaemons`
    - Runs `Updater` with the `CheckUpdate` parameter

`CelasTradePro` asks for the user's exchange and loads a legitimate-looking cryptocurrency trading platform—very similar to the benign Q.T. Bitcoin Trader—that exhibits no signs of malicious activity.

`Updater` checks for the `CheckUpdate` parameter and, when found, it collects the victim's host information (*System Owner/User Discovery* [T1033]), encrypts the collected information with a hardcoded XOR key before exfiltration, and sends the encrypted information to a C2 website (*Exfiltration Over C2 Channel* [T1041]). This process helps the adversary obtain persistence on a victim's network.

The `postinstall` script is a sequence of instructions that runs after successfully installing an application (*Command and Scripting Interpreter: Unix Shell* [T1059.004]). This script moves property list (`plist`) file `.com.celastradepro.plist` from the installer package to the `LaunchDaemons` folder (*Scheduled Task/Job: Launchd* [T1053.004]). The leading "." makes it unlisted in the Finder app or default Terminal directory listing (*Hide Artifacts: Hidden Files and Directories* [T1564.001]). Once in the folder, this property list (`plist`) file will launch the `Updater` program with the `CheckUpdate` parameter on system load as Root for every user. Because the `LaunchDaemon` will not run automatically after the `plist` file is moved, the `postinstall` script launches the `Updater` program with the `CheckUpdate` parameter and runs it in the background (Create or *Modify System Process: Launch Daemon* [T1543.004]).

Payload

After a cybersecurity company published a report detailing the above programs and their malicious extras, the website was no longer accessible. Since this site was the C2 server, the payload cannot be confirmed. The cybersecurity company that published the report states the payload was an encrypted and obfuscated binary (*Obfuscated Files or Information* [T1027]), which eventually drops FALLCHILL onto the machine and installs

it as a service (*Create or Modify System Process: Windows Service* [T1543.003]). FALLCHILL malware uses an RC4 encryption algorithm with a 16-byte key to protect its communications (*Encrypted Channel: Symmetric Cryptography* [T1573.001]). The key employed in these versions has also been used in a previous version of FALLCHILL.[5][6]

For more details on AppleJeus Version 1: Celas Trade Pro, see MAR-10322463-1.v1.

AppleJeus Version 2: JMT Trading

Introduction and Infrastructure

In October 2019, a cybersecurity company identified a new version of the AppleJeus malware—JMT Trading—thanks to its many similarities to the original AppleJeus malware. Again, the malware was in the form of a cryptocurrency trading application, which a legitimate-looking company, called JMT Trading, marketed and distributed on their website, `jmttrading[.]org` (*Acquire Infrastructure: Domain* [T1583.001]). This website contained a "Download from GitHub" button, which linked to JMT Trading's GitHub page (*Acquire Infrastructure: Web Services* [T1583.006]), where Windows and macOS X versions of the JMT Trader application were available for download (*Develop Capabilities: Malware* [T1587.001]). The GitHub page also included .zip and tar.gz files containing the source code.

The `jmttrading[.]org` domain resolved to the following IP addresses from October 15, 2016, to January 22, 2021.

- `45.33.2[.]79`
- `45.33.23[.]183`
- `45.56.79[.]23`
- `45.79.19[.]196`
- `96.126.123[.]244`
- `146.112.61[.]107`
- `184.168.221[.]40`
- `184.168.221[.]57`
- `198.187.29[.]20`
- `198.54.117[.]197`
- `198.54.117[.]198`
- `198.54.117[.]199`
- `198.54.117[.]200`
- `198.58.118[.]167`

The `jmttrading[.]org` domain had a valid Sectigo SSL certificate (*Obtain Capabilities: Digital Certificates* [T1588.004]). The SSL certificate was "Domain Control Validated," a weak security verification level that does not require validation of the owner's identity or the actual business's existence. The current SSL certificate was issued by Let's Encrypt.

JMT Trading Application Analysis

Windows Program

The Windows version of the malicious cryptocurrency application is an MSI Installer. The installer looks legitimate and has a valid digital signature from Sectigo (*Obtain Capabilities: Digital Certificates* [T1588.004]). The signature was signed with a code signing certificate purchased by the same user as the SSL certificate for `jmttrading[.]org` (*Obtain Capabilities: Code Signing Certificates* [T1588.003]). The MSI Installer asks the victim for administrative privileges to run (*User Execution: Malicious File* [T1204.002]).

Once permission is granted, the MSI executes the following actions.

- Installs `JMTTrader.exe` in folder `C:\Program Files (x86)\JMTTrader`
- Installs `CrashReporter.exe` in folder `C:\Users\<username>\AppData\Roaming\JMTTrader`
- Runs `CrashReporter.exe` with the `Maintain` parameter

The `JMTTrader.exe` program asks for the user's exchange and loads a legitimate-looking cryptocurrency trading platform—very similar to `CelasTradePro.exe` and the benign Q.T. Bitcoin Trader—that exhibits no signs of malicious activity.

The program `CrashReporter.exe` is heavily obfuscated with the ADVObfuscation library, renamed "snowman" (*Obfuscated Files or Information* [T1027]). When run, it checks for the `Maintain` parameter and collects the victim's host information (*System Owner/User Discovery* [T1033]), encrypts the collected information with a hardcoded XOR key before exfiltration, and sends the encrypted information to a C2 website (*Exfiltration Over C2 Channel* [T1041]). The program also creates a scheduled SYSTEM task, named `JMTCrashReporter`, which runs `CrashReporter.exe` with the `Maintain` parameter at any user's login (*Scheduled Task/Job: Scheduled Task* [T1053.005]).

macOS X Program

The macOS version of the malicious application is a DMG Installer. The installer looks legitimate and has very similar functionality to the Windows version, but it does not have a digital certificate and will warn the user of that before installation. The installer executes the following actions.

- Installs `JMTTrader` in folder `/Applications/JMTTrader.app/Contents/MacOS/`
- Installs `.CrashReporter` in folder `/Applications/JMTTrader.app/Contents/Resources/`
    - Note: the leading "." makes it unlisted in the Finder app or default Terminal directory listing.
- Executes a `postinstall` script
    - Moves `.com.jmttrading.plist` to folder `LaunchDaemons`
    - Changes the file permissions on the `plist`
    - Runs `CrashReporter` with the `Maintain` parameter
    - Moves `.CrashReporter` to folder `/Library/JMTTrader/CrashReporter`
    - Makes `.CrashReporter` executable

The `JMTTrader` program asks for the user's exchange and loads a legitimate-looking cryptocurrency trading platform—very similar to `CelasTradePro` and the benign Q.T. Bitcoin Trader—that exhibits no signs of malicious activity.

The `CrashReporter` program checks for the `Maintain` parameter and is not obfuscated. This lack of obfuscation makes it easier to determine the program's functionality in detail. When it finds the `Maintain` parameter, it collects the victim's host information (*System Owner/User Discovery* [T1033]), encrypts the collected information with a hardcoded XOR key before exfiltration, and sends the encrypted information to a C2 website (*Exfiltration Over C2 Channel* [T1041]).

The `postinstall` script has similar functionality to the one used by `CelasTradePro`, but it has a few additional features (*Command and Scripting Interpreter: Unix Shell* [T1059.004]). It moves the property list (`plist`) file `.com.jmttrading.plist` from the Installer package to the `LaunchDaemons` folder (*Scheduled Task/Job: Launchd* [T1053.004]), but also changes the file permissions on the `plist` file. Once in the folder, this property list (`plist`) file will launch the `CrashReporter` program with the `Maintain` parameter on system load as Root for every user. Also, the `postinstall` script moves the `.CrashReporter` program to a new location `/Library/JMTTrader/CrashReporter` and makes it executable. Because the `LaunchDaemon` will not run automatically after the `plist` file is moved, the `postinstall` script launches `CrashReporter` with the `Maintain` parameter and runs it in the background (*Create or Modify System Process: Launch Daemon* [T1543.004]).

Payload

Soon after the cybersecurity company tweeted about JMT Trader on October 11, 2019, the files on GitHub were updated to clean, non-malicious installers. Then on October 13, 2019, a different cybersecurity company published an article detailing the macOS X JMT Trader, and soon after, the C2 `beastgoc[.]com` website went offline. There is not a confirmed sample of the payload to analyze at this point.

For more details on AppleJeus Version 2: JMT Trading, see MAR-10322463-2.v1.

AppleJeus Version 3: Union Crypto

Introduction and Infrastructure

In December 2019, another version of the AppleJeus malware was identified on Twitter by a cybersecurity company based on many similarities to the original AppleJeus malware. Again, the malware was in the form of a cryptocurrency trading application, which was marketed and distributed by a legitimate-looking company, called Union Crypto, on their website, `unioncrypto[.]vip` (*Acquire Infrastructure: Domain* [T1583.001]). Although this website is no longer available, a cybersecurity researcher discovered a download link, `https://www.unioncrypto[.]vip/download/W6c2dq8By7luMhCmya2v97YeN`, recorded on VirusTotal for the macOS X version of `UnionCryptoTrader`. In contrast, open-source reporting stated that the Windows version might have been downloaded via instant messaging service Telegram, as it was found in a "Telegram Downloads" folder on an unnamed victim.[7]

The `unioncrypto[.]vip` domain resolved to the following IP addresses from June 5, 2019, to July 15, 2020.

- `104.168.167[.]16`
- `198.54.117[.]197`
- `198.54.117[.]198`

- `198.54.117[.]199`
- `198.54.117[.]200`

The domain `unioncrypto[.]vip` had a valid Sectigo SSL certificate (*Obtain Capabilities: Digital Certificates* [T1588.004]). The SSL certificate was "Domain Control Validated," a weak security verification level that does not require validation of the owner's identity or the actual business's existence.

Union Crypto Trader Application Analysis

Windows Program

The Windows version of the malicious cryptocurrency application is a Windows executable (`.exe`) (*User Execution: Malicious File* [T1204.002]), which acts as an installer that extracts a temporary MSI Installer.

The Windows program executes the following actions.

- Extracts `UnionCryptoTrader.msi` to folder `C:\Users\<username>\AppData\Local\Temp\{82E4B719-90F74BD1-9CF1-56CD777E0C42}`
- Runs `UnionCryptoUpdater.msi`
  - Installs `UnionCryptoTrader.exe` in folder `C:\Program Files\UnionCryptoTrader`
  - Installs `UnionCryptoUpdater.exe in folder C:\Users\<username>\AppData\Local\UnionCryptoTrader`
- Deletes `UnionCryptoUpdater.msi`
- Runs `UnionCryptoUpdater.exe`

The program `UnionCryptoTrader.exe` loads a legitimate-looking cryptocurrency arbitrage application—defined as "the simultaneous buying and selling of securities, currency, or commodities in different markets or in derivative forms to take advantage of differing prices for the same asset"—which exhibits no signs of malicious activity. This application is very similar to another cryptocurrency arbitrage application known as Blackbird Bitcoin Arbitrage.[8]

The program `UnionCryptoUpdater.exe` first installs itself as a service (*Create or Modify System Process: Windows Service* [T1543.003]), which will automatically start when any user logs on (*Boot or Logon Autostart Execution* [T1547]). The service is installed with a description stating it "Automatically installs updates for Union Crypto Trader." When launched, it collects the victim's host information (*System Owner/User Discovery* [T1033]), combines the information in a string that is MD5 hashed and stored in the `auth_signature` variable before exfiltration, and sends it to a C2 website (*Exfiltration Over C2 Channel* [T1041]).

macOS X Program

The macOS version of the malicious application is a DMG Installer. The installer looks legitimate and has very similar functionality to the Windows version, but it does not have a digital certificate and will warn the user of that before installation. The installer executes the following actions.

- Installs `UnionCryptoTrader` in folder `/Applications/UnionCryptoTrader.app/Contents/MacOS/`

- Installs `.unioncryptoupdater` in folder `/Applications/UnionCryptoTrader.app/Contents/Resources/`
  - Note: the leading "." makes it unlisted in the Finder app or default Terminal directory listing
- Executes a `postinstall` script
  - Moves `.vip.unioncrypto.plist` to folder `LaunchDaemons`
  - Changes the file permissions on the `plist` to Root
  - Runs `unioncryptoupdater`
  - Moves `.unioncryptoupdater` to folder `/Library/UnionCrypto/unioncryptoupdater`
  - Makes `.unioncryptoupdater` executable

The `UnionCryptoTrader` program loads a legitimate-looking cryptocurrency arbitrage application, which exhibits no signs of malicious activity. The application is very similar to another cryptocurrency arbitrage application known as Blackbird Bitcoin Arbitrage.

The `.unioncryptoupdater` program is signed ad-hoc, meaning it is not signed with a valid code-signing identity. When launched, it collects the victim's host information (*System Owner/User Discovery* [T1033]), combines the information in a string that is MD5 hashed and stored in the `auth_signature` variable before exfiltration, and sends it to a C2 website (*Exfiltration Over C2 Channel* [T1041]).

The `postinstall` script has similar functionality to the one used by JMT Trading (*Command and Scripting Interpreter: Unix Shell* [T1059.004]). It moves the property list (`plist`) file `.vip.unioncrypto.plist` from the Installer package to the `LaunchDaemons` folder (*Scheduled Task/Job: Launchd* [T1053.004]), but also changes the file permissions on the `plist` file to Root. Once in the folder, this property list (`plist`) file will launch the `.unioncryptoupdater` on system load as Root for every user. The `postinstall` script moves the `.unioncryptoupdater` program to a new location `/Library/UnionCrypto/unioncryptoupdater` and makes it executable. Because the `LaunchDaemon` will not run automatically after the `plist` file is moved, the `postinstall` script launches `.unioncryptoupdater` and runs it in the background (*Create or Modify System Process: Launch Daemon* [T1543.004]).

Payload

The payload for the Windows malware is a Windows Dynamic-Link-Library. `UnionCryptoUpdater.exe` does not immediately download the stage 2 malware but instead downloads it after a time specified by the C2 server. This delay could be implemented to prevent researchers from directly obtaining the stage 2 malware.

The macOS X malware's payload could not be downloaded, as the C2 server is no longer accessible. Additionally, none of the open-source reporting for this sample contained copies of the macOS X payload. The macOS X payload is likely similar in functionality to the Windows stage 2 detailed above.

For more details on AppleJeus Version 3: Union Crypto, see MAR-10322463-3.v1.

Commonalities between Celas Trade Pro, JMT Trading, and Union Crypto

Hardcoded Values

In each AppleJeus version, there are hardcoded values used for encryption or to create a signature when combined with the time (table 1).

Table 1: AppleJeus hardcoded values and uses

AppleJeus Version	Value	Use
1: Celas Trade Pro	Moz&Wie;#t/6T!2y	XOR encryption to send data
1: Celas Trade Pro	W29ab@ad%Df324V$Yd	RC4 decryption
2: JMT Trader Windows	X,%`PMk--Jj8s+6=15:20:11	XOR encryption to send data
2: JMT Trader OSX	X,%`PMk--Jj8s+6=\x02	XOR encryption to send data
3: Union Crypto Trader	12GWAPCT1F0I1S14	Combined with time for signature

The Union Crypto Trader and Celas LLC (XOR) values are 16 bytes in length. For JMT Trader, the first 16 bytes of the Windows and macOS X values are identical, and the additional bytes are in a time format for the Windows sample. The structure of a 16-byte value combined with the time is also used in Union Crypto Trader to create the `auth_signature`.

As mentioned, FALLCHILL was reported as the final payload for Celas Trade Pro. All FALLCHILL samples use 16-byte hardcoded RC4 keys for sending data, similar to the 16-byte keys in the AppleJeus samples.

Open-Source Cryptocurrency Applications

All three AppleJeus samples are bundled with modified copies of legitimate cryptocurrency applications and can be used as originally designed to trade cryptocurrency. Both Celas LLC and JMT Trader modified the same cryptocurrency application, Q.T. Bitcoin Trader; Union Crypto Trader modified the Blackbird Bitcoin Arbitrage application.

Postinstall Scripts, Property List Files, and LaunchDaemons

The macOS X samples of all three AppleJeus versions contain `postinstall` scripts with similar logic. The Celas LLC `postinstall` script only moves the `plist` file to a new location and launches `Updater` with the `CheckUpdate` parameter in the background. The JMT Trader and Union Crypto Trader also perform these actions and have identical functionality. The additional actions performed by both `postinstall` scripts are to change the file permissions on the `plist`, make a new directory in the `/Library` folder, move `CrashReporter` or `UnionCryptoUpdater` to the newly created folder, and make them executable.

The `plist` files for all three AppleJeus files have identical functionality. They only differ in the files' names and one default comment that was not removed from the Celas LLC `plist`. As the logic and functionality of the postinstall scripts and plist files are almost identical, the `LaunchDaemons` created also function the same.

They will all launch the secondary executable as Root on system load for every user.

AppleJeus Version 4: Kupay Wallet

Introduction and Infrastructure

On March 13, 2020, a new version of the AppleJeus malware was identified. The malware was marketed and distributed by a legitimate-looking company, called Kupay Wallet, on their website `kupaywallet[.]com` (*Acquire Infrastructure: Domain* [T1583.001]).

The domain `www.kupaywallet[.]com` resolved to IP address `104.200.67[.]96` from March 20, 2020, to January 16, 2021. CrownCloud US, LLC controlled the IP address (autonomous system number [ASN] 8100), and is located in New York, NY.

The domain `www.kupaywallet[.]com` had a valid Sectigo SSL certificate (*Obtain Capabilities: Digital Certificates* [T1588.004]). The SSL certificate was "Domain Control Validated," a weak security verification level that does not require validation of the owner's identity or the actual business's existence.

Kupay Wallet Application Analysis

Windows Program

The Windows version of the malicious cryptocurrency application is an MSI Installer. The MSI executes the following actions.

- Installs `Kupay.exe` in folder `C:\Program Files (x86)\Kupay`
- Installs `KupayUpgrade.exe` in folder `C:\Users\<username>\AppData\Roaming\KupaySupport`
- Runs `KupayUpgrade.exe`

The program `Kupay.exe` loads a legitimate-looking cryptocurrency wallet platform, which exhibits no signs of malicious activity and is very similar to an open-source platform known as Copay, distributed by Atlanta-based company BitPay.

The program `KupayUpgrade.exe` first installs itself as a service (*Create or Modify System Process: Windows Service* [T1543.003]), which will automatically start when any user logs on (*Boot or Logon Autostart Execution* [T1547]). The service is installed with a description stating it is an "Automatic Kupay Upgrade." When launched, it collects the victim's host information (*System Owner/User Discovery* [T1033]), combines the information in strings before exfiltration, and sends it to a C2 website (*Exfiltration Over C2 Channel* [T1041]).

macOS X Program

The macOS version of the malicious application is a DMG Installer. The installer looks legitimate and has very similar functionality to the Windows version, but it does not have a digital certificate and will warn the user of that before installation. The installer executes the following actions.

- Installs `Kupay` in folder `/Applications/Kupay.app/Contents/MacOS/`
- Installs `kupay_upgrade` in folder `/Applications/Kupay.app/Contents/MacOS/`
- Executes a `postinstall` script

- Creates `KupayDaemon` folder in `/Library/Application Support` folder
- Moves `kupay_upgrade` to the new folder
- Moves `com.kupay.pkg.wallet.plist` to folder `/Library/LaunchDaemons/`
- Runs the command `launchctl load` to load the `plist` without a restart
- Runs `kupay_upgrade` in the background

`Kupay` is likely a copy of an open-source cryptocurrency wallet application, loads a legitimate-looking wallet program (fully functional), and its functionality is identical to the Windows `Kupay.exe` program.

The `kupay_upgrade` program calls its function `CheckUpdate` (which contains most of the logic functionality of the malware) and sends a `POST` to the C2 server with a connection named "Kupay Wallet 9.0.1 (Check Update Osx)" (*Application Layer Protocol: Web Protocols* [T1071.001]). If the C2 server returns a file, it is decoded and written to the victim's folder `/private/tmp/kupay_update` with permissions set by the command `chmod 700` (only the user can read, write, and execute) (*Command and Scripting Interpreter* [T1059]). Stage 2 is then launched, and the malware, `kupay_upgrade` , returns to sleeping and checking in with the C2 server at predetermined intervals (*Application Layer Protocol: Web Protocols* [T1071.001]).

The `postinstall` script has similar functionality to other AppleJeus scripts (*Command and Scripting Interpreter: Unix Shell* [T1059.004]). It creates the `KupayDaemon` folder in `/Library/Application` Support folder and then moves `kupay_upgrade` to the new folder. It moves the property list (`plist`) file `com.kupay.pkg.wallet.plist` from the Installer package to the `/Library/LaunchDaemons/` folder (*Scheduled Task/Job: Launchd* [T1053.004]). The script runs the command `launchctl load` to load the `plist` without a restart (*Command and Scripting Interpreter* [T1059]). But, since the LaunchDaemon will not run automatically after the `plist` file is moved, the `postinstall` script launches `kupay_upgrade` and runs it in the background (*Create or Modify System Process: Launch Daemon* [T1543.004]).

Payload

The Windows malware's payload could not be downloaded since the C2 server is no longer accessible. Additionally, none of the open-source reporting for this sample contained copies of the payload. The Windows payload is likely similar in functionality to the macOS X stage 2 detailed below.

The stage 2 payload for the macOS X malware was decoded and analyzed. The stage 2 malware has a variety of functionalities. Most importantly, it checks in with a C2 and, after connecting to the C2, can send or receive a payload, read and write files, execute commands via the terminal, etc.

For more details on AppleJeus Version 4: Kupay Wallet, see MAR-10322463-4.v1.

AppleJeus Version 5: CoinGoTrade

Introduction and Infrastructure

In early 2020, another version of the AppleJeus malware was identified. This time the malware was marketed and distributed by a legitimate-looking company called CoinGoTrade on their website `coingotrade[.]com` (*Acquire Infrastructure: Domain* [T1583.001]).

The domain `CoinGoTrade[.]com` resolved to IP address `198.54.114[.]175` from February 28, 2020, to January 23, 2021. The IP address is controlled by NameCheap Inc. (ASN 22612) and is located in Atlanta, GA. This IP address is in the same ASN for `Dorusio[.]com` and `Ants2Whale[.]com`.

The domain `CoinGoTrade[.]com` had a valid Sectigo SSL certificate (*Obtain Capabilities: Digital Certificates* [T1588.004]). The SSL certificate was "Domain Control Validated," a weak security verification level that does not require validation of the owner's identity or the actual business's existence.

CoinGoTrade Application Analysis

Windows Program

The Windows version of the malicious application is an MSI Installer. The installer appears to be legitimate and will execute the following actions.

- Installs `CoinGoTrade.exe` in folder `C:\Program Files (x86)\CoinGoTrade`
- Installs `CoinGoTradeUpdate.exe` in folder `C:\Users\<username>\AppData\Roaming\CoinGoTradeSupport`
- Runs `CoinGoTradeUpdate.exe`

`CoinGoTrade.exe` loads a legitimate-looking cryptocurrency wallet platform with no signs of malicious activity and is a copy of an open-source cryptocurrency application.

`CoinGoTradeUpdate.exe` first installs itself as a service (*Create or Modify System Process: Windows Service* [T1543.003]), which will automatically start when any user logs on (*Boot or Logon Autostart Execution* [T1547]). The service is installed with a description stating it is an "Automatic CoinGoTrade Upgrade." When launched, it collects the victim's host information (*System Owner/User Discovery* [T1033]), combines the information in strings before exfiltration, and sends it to a C2 website (*Exfiltration Over C2 Channel* [T1041]).

macOS X Program

The macOS version of the malicious application is a DMG Installer. The installer looks legitimate and has very similar functionality to the Windows version, but it does not have a digital certificate and will warn the user of that before installation. The installer executes the following actions.

- Installs `CoinGoTrade` in folder `/Applications/CoinGoTrade.app/Contents/MacOS/`
- Installs `CoinGoTradeUpgradeDaemon` in folder `/Applications/CoinGoTrade.app/Contents/MacOS/`
- Executes a `postinstall` script
    - Creates `CoinGoTradeService` folder in `/Library/Application Support` folder
    - Moves `CoinGoTradeUpgradeDaemon` to the new folder
    - Moves `com.coingotrade.pkg.product.plist` to folder `/Library/LaunchDaemons/`
    - Runs `CoinGoTradeUpgradeDaemon` in the background

The `CoinGoTrade` program is likely a copy of an open-source cryptocurrency wallet application and loads a legitimate-looking, fully functional wallet program).

The `CoinGoTradeUpgradeDaemon` program calls its function `CheckUpdate` (which contains most of the logic functionality of the malware) and sends a `POST` to the C2 server with a connection named “CoinGoTrade 1.0 (Check Update Osx)” (*Application Layer Protocol: Web Protocols* [T1071.001]). If the C2 server returns a file, it is decoded and written to the victim’s folder `/private/tmp/updatecoingotrade` with permissions set by the command `chmod 700` (only the user can read, write, and execute) (*Command and Scripting Interpreter* [T1059]). Stage 2 is then launched, and the malware, `CoinGoTradeUpgradeDaemon` , returns to sleeping and checking in with the C2 server at predetermined intervals (*Application Layer Protocol: Web Protocols* [T1071.001]).

The `postinstall` script has similar functionality to the other scripts (*Command and Scripting Interpreter: Unix Shell* [T1059.004]) and installs `CoinGoTrade` and `CoinGoTradeUpgradeDaemon` in folder `/Applications/CoinGoTrade.app/Contents/MacOS/` . It moves the property list (plist) file `com.coingotrade.pkg.product.plist` to the `/Library/LaunchDaemons/` folder (*Scheduled Task/Job: Launchd* [T1053.004]). Because the `LaunchDaemon` will not run automatically after the `plist` file is moved, the `postinstall` script launches `CoinGoTradeUpgradeDaemon` and runs it in the background (*Create or Modify System Process: Launch Daemon* [T1543.004]).

Payload

The Windows malware’s payload could not be downloaded because the C2 server is no longer accessible. Additionally, none of the open-source reporting for this sample contained copies of the payload. The Windows payload is likely similar in functionality to the macOS X stage 2 detailed below.

The stage 2 payload for the macOS X malware was no longer available from the specified download URL. Still, a file was submitted to VirusTotal by the same user on the same date as the macOS X `CoinGoTradeUpgradeDaemon` . These clues suggest that the submitted file may be related to the macOS X version of the malware and the downloaded payload.

The file `prtspool` is a 64-bit Mach-O executable with a large variety of features that have all been confirmed as functionality. The file has three C2 URLs hardcoded into the file and communicates to these with HTTP POST multipart-form data boundary string. Like other HIDDEN COBRA malware, `prtspool` uses format strings to store data collected about the system and sends it to the C2s.

For more details on AppleJeus Version 5: CoinGoTrade, see MAR-10322463-5.v1.

AppleJeus Version 6: Dorusio

Introduction and Infrastructure

In March 2020, an additional version of the AppleJeus malware was identified. This time the malware was marketed and distributed by a legitimate-looking company called Dorusio on their website, `dorusio[.]com` (*Acquire Infrastructure: Domain* [T1583.001]). Researchers collected samples for Windows and macOS X versions of the Dorusio Wallet (*Develop Capabilities: Malware* [T1587.001]). As of at least early 2020, the actual download links result in `404` errors. The download page has release notes with version revisions claiming to start with version 1.0.0, released on April 15, 2019.

The domain dorusio[.]com resolved to IP address `198.54.115[.]51` from March 30, 2020 to January 23, 2021. The IP address is controlled by NameCheap Inc. (ASN 22612) and is located in Atlanta, GA. This IP address is in the same ASN for `CoinGoTrade[.]com` and `Ants2Whale[.]com.`

The domain `dorusio[.]com` had a valid Sectigo SSL certificate (*Obtain Capabilities: Digital Certificates* [T1588.004]). The SSL certificate was "Domain Control Validated," a weak security verification level that does not require validation of the owner's identity or the actual business's existence.

Dorusio Application Analysis

Windows Program

The Windows version of the malicious application is an MSI Installer. The installer appears to be legitimate and will install the following two programs.

- Installs `Dorusio.exe` in folder `C:\Program Files (x86)\Dorusio`
- Installs `DorusioUpgrade.exe` in folder `C:\Users\<username>\AppData\Roaming\DorusioSupport`
- Runs `DorusioUpgrade.exe`

The program, `Dorusio.exe`, loads a legitimate-looking cryptocurrency wallet platform with no signs of malicious activity and is a copy of an open-source cryptocurrency application.

The program `DorusioUpgrade.exe` first installs itself as a service (*Create or Modify System Process: Windows Service* [T1543.003]), which will automatically start when any user logs on (*Boot or Logon Autostart Execution* [T1547]). The service is installed with a description stating it "Automatic Dorusio Upgrade." When launched, it collects the victim's host information (*System Owner/User Discovery* [T1033]), combines the information in strings before exfiltration, and sends it to a C2 website (*Exfiltration Over C2 Channel* [T1041]).

macOS X Program

The macOS version of the malicious application is a DMG Installer. The installer looks legitimate and has very similar functionality to the Windows version, but it does not have a digital certificate and will warn the user of that before installation. The installer executes the following actions.

- Installs `Dorusio` in folder `/Applications/Dorusio.app/Contents/MacOS/`
- Installs `Dorusio_upgrade` in folder `/Applications/Dorusio.app/Contents/MacOS/`
- Executes a `postinstall` script
    - Creates `DorusioDaemon` folder in `/Library/Application Support` folder
    - Moves `Dorusio_upgrade` to the new folder
    - Moves `com.dorusio.pkg.wallet.plist` to folder `/Library/LaunchDaemons/`
    - Runs `Dorusio_upgrade` in the background

The `Dorusio` program is likely a copy of an open-source cryptocurrency wallet application and loads a legitimate-looking wallet program (fully functional). Aside from the Dorusio logo and two new services, the

wallet appears to be the same as the Kupay Wallet. This application seems to be a modification of the open-source cryptocurrency wallet Copay distributed by Atlanta-based company BitPay.

The `Dorusio_upgrade` program calls its function `CheckUpdate` (which contains most of the logic functionality of the malware) and sends a `POST` to the C2 server with a connection named "*Dorusio Wallet 2.1.0 (Check Update Osx)*" (*Application Layer Protocol: Web Protocols* [T1071.001]). If the C2 server returns a file, it is decoded and written to the victim's folder `/private/tmp/Dorusio_update` with permissions set by the command `chmod 700` (only the user can read, write, and execute) (*Command and Scripting Interpreter* [T1059]). Stage 2 is then launched, and the malware, `Dorusio_upgrade`, returns to sleeping and checking in with the C2 server at predetermined intervals (*Application Layer Protocol: Web Protocols* [T1071.001]).

The `postinstall` script has similar functionality to other AppleJeus scripts (*Command and Scripting Interpreter: Unix Shell* [T1059.004]). It creates the `DorusioDaemon` folder in `/Library/Application Support` folder and then moves `Dorusio_upgrade` to the new folder. It moves the property list (`plist`) file `com.dorusio.pkg.wallet.plist` from the Installer package to the `/Library/LaunchDaemons/` folder (*Scheduled Task/Job: Launchd* [T1053.004]). Because the `LaunchDaemon` will not run automatically after the `plist` file is moved, the `postinstall` script launches `Dorusio_upgrade` and runs it in the background (*Create or Modify System Process: Launch Daemon* [T1543.004]).

Payload

Neither the payload for the Windows nor macOS X malware could be downloaded; the C2 server is no longer accessible. The payloads are likely similar in functionality to the macOS X stage 2 from CoinGoTrade and Kupay Wallet, or the Windows stage 2 from Union Crypto.

For more details on AppleJeus Version 6: Dorusio, see MAR-10322463-6.v1.

AppleJeus 4, 5, and 6 Installation Conflictions

If a user attempts to install the Kupay Wallet, CoinGoTrade, and Dorusio applications on the same system, they will encounter installation conflicts.

If Kupay Wallet is already installed on a system and the user tries to install CoinGoTrade or Dorusio:

- Pop-up windows appear, stating a more recent version of the program is already installed.

If CoinGoTrade is already installed on a system and the user attempts to install Kupay Wallet:

- `Kupay.exe` will be installed in the `C:\Program Files (x86)\CoinGoTrade\ folder`.
- All `CoinGoTrade` files will be deleted.
- The folders and files contained in the `C:\Users\<username>\AppData\Roaming\CoinGoTradeSupport` will remain installed.
- `KupayUpgrade.exe` is installed in the new folder `C:\Users\<username>\AppData\Roaming\KupaySupport`.

If Dorusio is already installed on a system and the user attempts to install Kupay Wallet:

- `Kupay.exe` will be installed in the `C:\Program Files (x86)\Dorusio\ folder`.
- All `Dorusio.exe` files will be deleted.
- The folders and files contained in `C:\Users\<username>\AppData\Roaming\DorusioSupport` will remain installed.
- `KupayUpgrade.exe` is installed in the new folder `C:\Users\<username>\AppData\Roaming\KupaySupport`.

AppleJeus Version 7: Ants2Whale

Introduction and Infrastructure

In late 2020, a new version of AppleJeus was identified called "Ants2Whale." The site for this version of AppleJeus is `ants2whale[.]com` (*Acquire Infrastructure: Domain* [T1583.001]). The website shows a legitimate-looking cryptocurrency company and application. The website contains multiple spelling and grammar mistakes indicating the creator may not have English as a first language. The website states that to download Ants2Whale, a user must contact the administrator, as their product is a "premium package" (*Develop Capabilities: Malware* [T1587.001]).

The domain `ants2whale[.]com` resolved to IP address `198.54.114[.]237` from September 23, 2020, to January 22, 2021. The IP address is controlled by NameCheap, Inc. (ASN 22612) and is located in Atlanta, GA. This IP address is in the same ASN for `CoinGoTrade[.]com` and `Dorusio[.]com`.

The domain `ants2whale[.]com` had a valid Sectigo SSL certificate (*Obtain Capabilities: Digital Certificates* [T1588.004]). The SSL certificate was "Domain Control Validated," a weak security verification level that does not require validation of the owner's identity or the actual business's existence.

Ants2Whale Application Analysis

Windows Program

As of late 2020, the Windows program was not available on VirusTotal. It is likely very similar to the macOS X version detailed below.

macOS X Program

The macOS version of the malicious application is a DMG Installer. The installer looks legitimate and has very similar functionality to the Windows version, but it does not have a digital certificate and will warn the user of that before installation. The installer executes the following actions.

- Installs `Ants2Whale` in folder `/Applications/Ants2whale.app/Contents/MacOS/Ants2whale`
- Installs `Ants2WhaleHelper` in folder `/Library/Application Support/Ants2WhaleSupport/`
- Executes a `postinstall` script
    - Moves `com.Ants2whale.pkg.wallet.plist` to folder `/Library/LaunchDaemons/`
    - Runs `Ants2WhaleHelper` in the background

The `Ants2Whale` and `Ants2WhaleHelper` programs and the `postinstall` script function almost identically to previous versions of AppleJeus and will not be discussed in depth in this advisory.

For more details on AppleJeus Version 7: Ants2Whale, see MAR-10322463-7.v1.

ATT&CK Profile

Figure 2 and table 2 provide summaries of the MITRE ATT&CK techniques observed.

Figure 2: MITRE ATT&CK enterprise techniques used by AppleJeus

Table 2: MITRE ATT&CK techniques observed

Tactic Title	Technique ID	Technique Title
Resource Development [TA0042]	T1583.001	Acquire Infrastructure: Domain
Resource Development [TA0042]	T1583.006	Acquire Infrastructure: Web Services
Resource Development [TA0042]	T1587.001	Develop Capabilities: Malware
Resource Development [TA0042]	T1588.003	Obtain Capabilities: Code Signing Certificates
Resource Development [TA0042]	T1588004	Obtain Capabilities: Digital Certificates
Initial Access [TA0001]	T1566.002	Phishing: Spearphishing Link
Execution [TA0002]	T1059	Command and Scripting Interpreter
Execution [TA0002]	T1059.004	Command and Scripting Interpreter: Unix Shell
Execution [TA0002]	T1204.002	User Execution: Malicious File
Persistence [TA0003]	T1053.004	Scheduled Task/Job: Launchd
Persistence [TA0003]	T1543.004	Create or Modify System Process: Launch Daemon
Persistence [TA0003]	T1547	Boot or Logon Autostart Execution
Privilege Escalation [TA0004]	T1053.005	Scheduled Task/Job: Scheduled Task
Defense Evasion [TA0005]	T1027	Obfuscated Files or Information
Defense Evasion [TA0005]	T1548	Abuse Elevation Control Mechanism
Defense Evasion [TA0005]	T1564.001	Hide Artifacts: Hidden Files and Directories
Discovery [TA0007]	T1033	System Owner/User Discovery
Exfiltration [TA0010]	T1041	Exfiltration Over C2 Channel
Command and Control [TA0011]	T1071.001	Application Layer Protocol: Web Protocols

Tactic Title	Technique ID	Technique Title
Command and Control [TA0011]	T1573	Encrypted Channel
Command and Control [TA0011]	T1573.001	Encrypted Channel: Symmetric Cryptography

Mitigations

Compromise Mitigations

Organizations that identify AppleJeus malware within their networks should take immediate action. Initial actions should include the following steps.

- Contact the FBI, CISA, or Treasury immediately regarding any identified activity related to AppleJeus. (Refer to the Contact Information section below.)
- Initiate your organization's incident response plan.
- Generate new keys for wallets, and/or move to new wallets.
- Introduce a two-factor authentication solution as an extra layer of verification.
- Use hardware wallets, which keep the private keys in a separate, secured storage area.
- To move funds out off a compromised wallet:
    - Do not use the malware listed in this advisory to transfer funds, and
    - Form all transactions offline and then broadcast them to the network all at once in a short online session, ideally prior to the attacker accessing them.
- Remove impacted hosts from network.
- Assume the threat actors have moved laterally within the network and downloaded additional malware.
- Change all passwords to any accounts associated with impacted hosts.
- Reimage impacted host(s).
- Install anti-virus software to run daily deep scans of the host.
- Ensure your anti-virus software is setup to download the latest signatures daily.
- Install a Host Based Intrusion Detection (HIDS)-based software and keep it up to date.
- Ensure all software and hardware is up to date, and all patches have been installed.
- Ensure network-based firewall is installed and/or up to date.
- Ensure the firewall's firmware is up to date.

Pro-Active Mitigations

Consider the following recommendations for defense against AppleJeus malware and related activity.

Cryptocurrency Users

- Verify source of cryptocurrency-related applications.
- Use multiple wallets for key storage, striking the appropriate risk balance between hot and cold storage.
- Use custodial accounts with multi-factor authentication mechanisms for both user and device verification.

- Patronize cryptocurrency service businesses that offer indemnity protections for lost or stolen cryptocurrency.
- Consider having a dedicated device for cryptocurrency management.

Financial Service Companies

- Verify compliance with Federal Financial Institutions Examination Council (FFIEC) handbooks at https://ithandbook.ffiec.gov, especially those related to information security.
- Report suspicious cyber and financial activities. For more information on mandatory and voluntary reporting of cyber events via suspicious activity reports, see the Financial Crimes Enforcement Network (FinCEN) Advisory FIN-2016-A005: Advisory to Financial Institutions on Cyber- Events and Cyber-Enabled Crime at https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf and FinCEN's Section 314(b) Fact Sheet at https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

Cryptocurrency Businesses

- Verify compliance with the Cryptocurrency Security Standard at http://cryptoconsortium.github.io/CCSS/ .

All Organizations

- Incorporate IOCs identified in CISA's Malware Analysis Reports on https://us-cert.cisa.gov/northkorea into intrusion detection systems and security alert systems to enable active blocking or reporting of suspected malicious activity.
- See table 3 below, which provides a summary of preventative ATT&CK mitigations based on observed techniques.

Table 3: MITRE ATT&CK mitigations based on observed techniques

Mitigation	Description
User Training [M1017]	Train users to identify social engineering techniques and spearphishing emails.
User Training [M1017]	Provide users with the awareness of common phishing and spearphishing techniques and raise suspicion for potentially malicious events.
User Account Management [M1018]	Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create new Launch Daemons.
User Account Management [M1018]	Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems.

Mitigation	Description
SSL/TLS Inspection [M1020]	Use SSL/TLS inspection to see encrypted sessions' contents to look for network-based indicators of malware communication protocols.
Restrict Web-Based Content [M1021]	Determine if certain websites that can be used for spearphishing are necessary for business operations and consider blocking access if the activity cannot be monitored well or poses a significant risk.
Restrict Web-Based Content [M1021]	Block Script extensions to prevent the execution of scripts and HTA files that may commonly be used during the exploitation process.
Restrict Web-Based Content [M1021]	Employ an adblocker to prevent malicious code served up through ads from executing.
Restrict File and Directory Permissions [M1022]	Prevent all users from writing to the `/Library/StartupItems` directory to prevent any startup items from getting registered since `StartupItems` are deprecated.
Privileged Account Management [M1026]	When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.
Privileged Account Management [M1026]	Configure the Increase Scheduling Priority option only to allow the Administrators group the rights to schedule a priority process.
Operating System Configuration [M1028]	Configure settings for scheduled tasks to force tasks to run under the authenticated account's context instead of allowing them to run as SYSTEM.
Network Intrusion Prevention [M1031]	Use network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware and mitigate activity at the network level.
Execution Prevention [M1038]	Use application control tools where appropriate.
Execution Prevention [M1038]	Use application control tools to prevent the running of executables masquerading as other files.
Behavior Prevention on Endpoint [M1040]	Configure endpoint (if possible) to block some process injection types based on common sequences of behavior during the injection process.
Disable or Remove Feature or Program [M1042]	Disable or remove any unnecessary or unused shells or interpreters.
Code Signing [M1045]	Where possible, only permit the execution of signed scripts.

Mitigation	Description
Audit [M1047]	Audit logging for `launchd` events in macOS can be reviewed or centrally collected using multiple options, such as Syslog, OpenBSM, or OSquery.
Audit [M1047]	Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges.
Antivirus/Antimalware [M1049]	Use an antivirus program to quarantine suspicious files automatically.

Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat.

For any questions related to this report or to report an intrusion and request resources for incident response or technical assistance, please contact:

- The FBI through the FBI Cyber Division (855-292-3937 or CyWatch@fbi.gov) or a local field office,
- CISA (1-844-Say-CISA or Central@cisa.dhs.gov), or
- Treasury Office of Cybersecurity and Critical Infrastructure Protection (Treasury OCCIP) (202-622-3000 or OCCIP-Coord@treasury.gov).

References

[6] MITRE ATT&CK Software: FALLCHILL

[7] SecureList: Operation AppleJeus Sequel

[8] GitHub: Blackbird Bitcoin Arbitrage

Revisions

February 17, 2021: Initial Version|April 15, 2021: Updated MITRE ATT&CK technique from Command and Scripting Interpreter: AppleScript [T1059.002] to Command and Scripting Interpreter: Unix Shell [T1059.004].
